

Appl. No.: 10/749,042
Amdt. dated 01/11/2006
Reply to Official Action of October 11, 2005

BEST AVAILABLE COPY

REMARKS/ARGUMENTS

This Reply is being filed in response to the second non-final Official Action of October 11, 2005, in which independent Claims 1, 7 and 13 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,224,163 to Gasser et al. As explained below, however, Applicant respectfully submits that the claimed invention is patentably distinct from Gasser, and accordingly traverses the rejection of the claims as being anticipated thereby. In view of the following remarks, Applicant respectfully requests reconsideration and allowance of all of the pending claims of the present application.

Initially, Applicant notes the Official Action's failure to substantively treat any of dependent Claims 2-6, 8-12 and 14-18. Accordingly, and by virtue of the failure of Gasser to teach or suggest any of the features claimed thereby, Applicant presumes that dependent Claims 2-6, 8-12 and 14-18 are allowable, and therefore respectfully requests an indication of such in the next Official Action.

As to the rejection of independent Claims 1, 7 and 13, Applicant notes that the Gasser patent discloses a system and method for delegating authorization from one entity to another within a distributed network. In those passages cited in the Official Action as disclosing the claimed invention, a user P (user principal) may initiate a computing session by authenticating to a workstation W1 (system principal), and vice versa. In many situations during a computing session, after the user and workstation authenticate to one another, the user may desire to access the resource of another destination workstation W_S (system principal) in a manner requiring communication via one or more intermediary workstations W2 (system principals). In such instances, authority of the user to access the resource of the destination workstation may be established via a chained delegation of authority of the user through the intermediary workstations to the destination workstation, which certifies the user's authority via delegation certificates of each intermediary workstation back to the user.

As more particularly disclosed by Gasser, to access the resource of a workstation W_S via a workstation W1 and an intermediary workstation W2, the user (or smart card associated with the user) signs a delegation certificate D1 indicating that workstation W1 is authorized to speak for the user, and provide, the delegation certificate D1 to workstation W1. In turn, workstation

Appl. No.: 10/749,042
Amdt. dated 01/11/2006
Reply to Official Action of October 11, 2005

BEST AVAILABLE COPY

W1 itself signs a delegation certificate D2 indicating that workstation W2 is authorized to speak for workstation W1, and provides both delegation certificates D1 and D2, as well as an authentication certificate of user P, to workstation W2. Workstation W2 then requests access to the resource of workstation W₃ using delegation certificates D1 and D2, and the authentication certificate of user P, to establish the authority of user P (via workstations W1 and W2) to access the resource of workstation W₃.

As previously explained, in accordance with one aspect of the claimed invention of the present application, as currently recited by independent Claim 1, a system is provided that includes a terminal, a secondary certification authority (CA), a tertiary CA and a server. As recited, the terminal is included within an organization including a plurality of terminals, where at least one terminal has at least one characteristic and is at one or more of a plurality of positions within an organization. The organization includes a plurality of secondary CA's capable of issuing role certificates to respective groups of terminals of the organization, and includes a plurality of tertiary CA's capable of issuing permission certificates to respective sub-groups of terminals of the organization. In this regard, the secondary CA is capable of providing at least one role certificate to the terminal based upon the position of the terminal within the organization. The tertiary CA, on the other hand, is capable of providing at least one permission certificate to the terminal based upon the characteristics of the respective terminal. Thus, the server is capable of authenticating the terminal based upon an identity certificate, the role certificate and the permission certificate of the terminal to thereby determine whether to grant the terminal access to at least one resource of the server.

As described above, Gasser and the claimed invention both generally relate to use of certificates to authenticate a computing device. In contrast to independent Claim 1, however, Gasser does not teach or suggest (i) a secondary CA providing role certificate(s) to a terminal based upon position(s) of the terminal within an organization; (ii) a tertiary CA providing permission certificate(s) to the terminal based upon characteristic(s) of the terminal at a position in the organization; and (iii) a server authenticating the terminal based upon an identity certificate, the role certificate(s) and the permission certificate(s).

Appl. No.: 10/749,042
Amdt. dated 01/11/2006
Reply to Official Action of October 11, 2005

BEST AVAILABLE COPY

A. *Providing Role Certificate(s)*

The Official Action appears to assert that Gasser's disclosure directed to providing a user with a smart card for authenticating the user corresponds to the recited feature of providing role certificate(s) to a terminal (aforementioned feature (i)), citing column 12, lines 43-66 of Gasser. As further disclosed by that passage of Gasser, upon providing the user with the smart card, the smart card issues information to a workstation such that the workstation retrieves certificates based on the information, and authenticates the user based upon those certificates. Even if one could interpret these disclosed certificates being provided to a workstation as corresponding to providing certificates to a terminal, as recited by the claimed invention, nowhere does Gasser teach or suggest that those certificates correspond to role certificate(s) provided based upon position(s) of the workstation within an organization, as also recited by the claimed invention. In fact, Gasser does not teach or suggest any basis for the provision of those certificates other than to authenticate the user to access resources of the workstation. Even considering this basis, however, the certificates are provided to the workstation irrespective of the workstation's position in an organization.

B. *Providing Permission Certificate(s)*

For the recited feature of a tertiary CA providing permission certificate(s) to the terminal (aforementioned feature (ii)), then, the Examiner cites a passage of Gasser directed to providing delegation certificates to workstations to speak for other workstations or users, citing column 13, line 23 – column 14, line 5. As indicated above, Gasser discloses that a user can authorize a workstation to speak on the user's behalf via a delegation certificate provided by the user to that workstation. Again, similar to the provision of certificates to the workstation to authenticate the user, Gasser does not teach or suggest that the delegation certificate is provided to the workstation based upon based upon characteristic(s) of the workstation at a position in the organization, similar to the permission certificate(s) of the claimed invention. Rather, the delegation certificate is provided to authorize the workstation to speak on the user's behalf, irrespective of any characteristic(s) of the workstation. Further, Gasser does not teach or suggest the user providing delegation certificate(s) to sub-groups of workstations, similar to the provision

Appl. No.: 10/749,042
Amdt. dated 01/11/2006
Reply to Official Action of October 11, 2005

BEST AVAILABLE COPY

of permission certificate(s) within the organization of the claimed invention. The user may provide a delegation certificate to a workstation, which itself provides that certificate and another delegation certificate to an intermediary workstation. Even in that instance, however, each entity provides delegation certificate(s) only to its most immediately adjacent workstation in the chain of communication, as opposed to providing delegation certificate(s) to a sub-group of workstations, similar to the claimed invention.

C. Authenticating a Terminal Based on Identity, Role and Permission Certificates

Finally, for the recited feature of authenticating the terminal based upon an identity certificate, the role certificate(s) and the permission certificate(s) (aforementioned feature (iii)), the Official Action again cites the passage of Gasser directed to delegation certificates, and particularly column 14, lines 5-18. Again, as explained above, Gasser discloses that in a number of situations, a user may desire to access the resources of a workstation W_3 via workstations W_1 and W_2 . In those situations, after providing delegation certificates D_1 and D_2 to workstations W_1 and W_2 , respectively, workstation W_2 requests access to the resource of workstation W_3 using delegation certificates D_1 and D_2 , and the authentication certificate of user P , to establish the authority of user P (via workstations W_1 and W_2) to access the resource of workstation W_3 . Initially, it should be noted that the certificate of Gasser being attributed to the role certificate appears to more accurately correspond to the recited identity certificate. And with both delegation certificates D_1 and D_2 being provided to workstations W_1 and W_2 , respectively, on the same basis (i.e., grant authority to speak on behalf of an immediately preceding principal), Gasser at best discloses two types of certificates upon which an entity is authenticated to access the resources of another principal. The claimed invention, on the other hand, authenticates an entity based upon three types of certificates, i.e., identity certificate, role certificate and permission certificate.

The Official Action appears to equate delegation certificates D_1 and D_2 to role and permission certificates, respectively. As disclosed by Gasser, delegation certificate D_1 is provided by the user to workstation W_1 , and delegation certificate D_2 is provided by workstation W_1 to another workstation W_2 . In accordance with the claimed invention, however, the role and

Appl. No.: 10/749,042
Amdt. dated 01/11/2006
Reply to Official Action of October 11, 2005

BEST AVAILABLE COPY

permission certificates are both provided to the same, recited terminal. Applicant notes that Gasser does disclose that workstation W1 passes its delegation certificate D1 to workstation W2 along with the delegation certificate D2 for workstation W2. Even considering this aspect of Gasser, however, delegation certificates D1 and D2 still cannot reasonably correspond to the recited role and permission certificate(s). In this regard, although workstation W1 passes both delegation certificates D1 and D2 to workstation W2, only delegation certificate D2 is passed with any basis to workstation W2 (i.e., authorizing W2 to speak on behalf of W1); delegation certificate D1, as indicated above, merely authorizing W1 to speak on behalf of user P. In accordance with the claimed invention, however, both the role and permission certificates are provided with basis to the recited terminal, the role certificate(s) being provided based upon position(s) of the terminal, and the permission certificate(s) being provided based upon characteristic(s) of the terminal.

Accordingly, Applicant respectfully submits that the claimed invention of independent Claim 1, and by dependency Claims 2-6, is patentably distinct from Gasser. Applicant also respectfully submits that independent Claims 7 and 13 recite subject matter similar to independent Claim 1. For example, independent Claims 7 and 13 recite providing a role certificate and a permission certificate, and authenticating a terminal based upon those certificates as well as an identity certificate. Accordingly, Applicant respectfully submits that the claimed invention of independent Claims 7 and 13, and by dependency Claims 8-12 and 14-18, is patentably distinct from Gasser for at least the same reasons given above with respect to independent Claim 1. Applicant therefore respectfully submits that the rejection of independent Claims 1, 7 and 13 under 35 U.S.C. § 102(b) as being anticipated by Gasser is overcome.


Appl. No.: 10/749,042
Amdt. dated 01/11/2006
Reply to Official Action of October 11, 2005

BEST AVAILABLE COPY**CONCLUSION**

In view of the remarks presented above, Applicant respectfully submits that the present application is in condition for allowance. As such, the issuance of a Notice of Allowance is therefore respectfully requested. In order to expedite the examination of the present application, the Examiner is encouraged to contact Applicant's undersigned attorney in order to resolve any remaining issues.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,




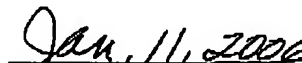
Andrew T. Spence
Registration No. 45,699

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that this paper is being facsimile transmitted to the US Patent and Trademark Office at Fax No. (571) 273-8800 on the date shown below.


Sarah B. Simmons


Date